UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,027	04/11/2001	Randall James Graham	MCVLT.001A	8350

20995 7590 08/17/2004

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER
PARTHASARATHY, PRAMILA

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/833,027	**Applicant(s)** GRAHAM, RANDALL JAMES	
	Examiner Pramila Parthasarathy	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 August 2002*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *7/01, 4/02 & 8/02* .

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 08/06/2002. Claims 1 – 43 were received for consideration. No preliminary amendments to the claims were filed. Claims 1 – 43 are currently being considered.

2. Three initialed and dated copies of Applicant's IDS form 1449 are attached to the Office action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1- 43 are rejected under 35 U.S.C. 102(e) as being anticipated by Olkin et al. (Patent Number 6,584,564).

Regarding Claim 1, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), comprising:

a form for entry of a password by a recipient of the document, the form being adapted to be displayed within an HTML-compliant web browser (Column 12 lines 21 – 56);

an encrypted message (Column 12 line 21 – Column 13 line 52); and

a decryption module that uses the password to decrypt the encrypted message for display within the HTML-compliant web browser (Column 15 lines 9 – 51);

wherein the document allows the encrypted message to be decrypted and viewed on a computer having an HTML-compliant browser installed thereon, without a need for decryption software installed on the computer (Column 15 line 31 – Column 17 line 4).

Regarding Claim 13, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28) comprising:

a document wrapper including a description of a user interface (Column 12 lines 21 – 56);

encrypted data representing a source message which has been encrypted with an encryption key (Column 12 line 21 – Column 13 line 52);

processing instructions located within the document wrapper (Column 12 lines 21 – 56; and

a decryption element configured to receive a password entered by a recipient via the user interface, and to use the password and the processing instructions to decrypt the encrypted data within the document (Column 15 lines 31 – 51).

Regarding Claim 30, Olkin teaches and describes, a secure messaging system for protecting the contents of an electronic message being sent to a recipient (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), the system comprising:

an encrypting module for preparing a secure document, the encrypting module configured to receive a key and an electronic message (Column 11 line 44 – Column 13line 52); and

an electronic mail gateway module configured to receive the secure document from the encrypting module and to send the secure document to a recipient, wherein the encrypting module is configured to create an encrypted message by encrypting the electronic message with the key, and wherein the secure document comprises an HTML-compliant wrapper, the encrypted message, a processing script, and a decryption element, the processing script containing instructions for accessing the encrypted message, and the decryption element being capable of recovering the electronic message from the encrypted message when presented with a password by the recipient (Fig. 1; Column 5 line

35 – Column 7 line 25; Column 12 line 21 – Column 13 line 52 and Column 15 lines 31 – 51).

Regarding Claim 33, Olkin teaches and describes, a method for sending a message to a recipient (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), the method comprising the steps of:

preparing an encrypted message by encrypting a source message using an encryption key and an encryption algorithm (Column 2 lines 6 – 49 and Column 12 line 21 – Column 13 line 52);

preparing a secure document comprising an HTML-compliant wrapper, the encrypted message, a processing script, and a decryption element, wherein the processing script contains instructions for accessing the encrypted message, and wherein the decryption element includes a module capable of recovering the source message from the encrypted message when presented with a password by the recipient (Column 12 lines 21 – 56 and Column 15 line 9 – Column 17 line 4); and

sending the secure document to a recipient (Column 13 lines 7 – 52).

Regarding Claim 38, Olkin teaches and describes, a method for sending and receiving a message (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), the method comprising the steps of:

preparing an encrypted message by encrypting a source message using an encryption key associated with a recipient and an encryption algorithm (Column 2 lines 6 – 49 and Column 12 line 21 – Column 13 line 52);

preparing a secure document comprising an HTML-compliant wrapper, the encrypted message, a processing script, and a decryption element (Column 12 line 21 – Column 13 line 52);

forwarding the secure document to a recipient's device (Column 13 line 7 – 52);

processing the wrapper of the secure document using a browser running on the recipient's device (Column 15 lines 31 – 51);

entering a password into the browser (Column 15 line 31 – 58);

running the processing script of the secure document to access the decryption element (Column 15 line 31 – Column 16 line 31);

recovering the source message by decrypting the encrypted message with the password and the decryption element (Column 16 lines 29 – 55); and

presenting the recovered source message to the recipient, wherein the secure document allows the encrypted message to be decrypted and viewed on a device having a browser installed thereon, without a need for decryption software installed on the device (Column 15 line 31 – 51 and Column 16 line 43 – 46).

Regarding Claim 43, Olkin teaches and describes, a computer readable medium having stored therein a software module (Fig. 1, 7; Column 3 line 32 –

Column 4 line 57 and Column 12 line 21 – Column 18 line 28), which when executed performs the steps of:

preparing an encrypted message by encrypting a source message using an encryption key and an encryption algorithm (Column 2 lines 6 – 49 and Column 12 line 21 – Column 13 line 52);

preparing a secure document comprising an HTML-compliant wrapper, the encrypted message, a processing script, and a decryption element, wherein the processing script contains instructions for accessing the encrypted message, and wherein the decryption element includes a module capable of recovering the source message from the encrypted message when presented with a password by the recipient (Column 12 lines 21 – 56 and Column 15 line 9 – Column 17 line 4);

forwarding the secure document to a mail gateway module (Column 13 line 7 – 52).

Claims 2, 14, 16 and 17 are rejected as applied above in rejecting claims 1 and 13. Furthermore, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the form is configured to present a password entry field and a decryption button to a user when the form is processed by the HTML-compliant web browser (Column 3 lines 42 – 50 and Column 15 lines 1 – 44).

Claims 3 and 19 are rejected as applied above in rejecting claims 1 and 13. Furthermore, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the encrypted message comprises an email attachment (Column 13 line 7 – Column 14 line 35).

Claims 4 and 20 are rejected as applied above in rejecting claims 1 and 13. Furthermore, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the decryption module comprises script code configured to be executed within the HTML-compliant browser (Column 15 line 31 – Column 17 line 4).

Claims 7 and 23 are rejected as applied above in rejecting claims 1 and 13. Furthermore, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the decryption module is configured to receive a password and use the password to generate a decryption key, the decryption module being configured to use the decryption key to decrypt the encrypted message (Column 15 line 31 – Column 17 line 4).

Claims 8 and 25 are rejected as applied above in rejecting claims 1 and 13. Furthermore, Olkin teaches and describes, a secure electronic document

(Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the decryption module comprises an Active X control (Column 15 lines 9 – 15 and column 18 line 60 – Column 19 line 6).

Claims 9 and 26 are rejected as applied above in rejecting claims 1 and 13. Furthermore, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the decryption module comprises software which is configured to be executed within a browser (Column 7 line 47 – Column 8 line 67).

Claims 10 and 27 are rejected as applied above in rejecting claims 1 and 13. Furthermore, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the decryption module is downloaded across a communications medium as needed (Column 7 line 47 – Column 8 line 67).

Claims 11 and 28 are rejected as applied above in rejecting claims 1 and 13. Furthermore, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the decryption module comprises a Java applet (Column 7 line 47 – Column 8 line 67).

Claims 12 and 29 are rejected as applied above in rejecting claims 1 and 13. Furthermore, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the decryption module comprises both a Java program and an Active X control (Column 7 line 47 – Column 8 line 67).

Claims 15, 34, 37, 39 and 42 are rejected as applied above in rejecting claims 13, 33 and 38. Furthermore, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the document wrapper is formatted in Extensible Markup Language (Column 12 lines 57 – 65).

Claim 31 is rejected as applied above in rejecting claim 30. Furthermore, Olkin teaches and describes, a secure messaging system for protecting the contents of an electronic message being sent to a recipient (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the decryption element is configured to send a confirmation message to the encrypting module confirming the successful access of the encrypted message by the recipient (Column 13 lines 7 – 52).

Claims 5, 21 and 24 are rejected as applied above in rejecting claims 4 and 13. Furthermore, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column

18 line 28), wherein the decryption module comprises JavaScript commands (Column 7 line 47 – Column 8 line 67).

Claims 6 and 22 are rejected as applied above in rejecting claims 4 and 13. Furthermore, Olkin teaches and describes, a secure electronic document (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the decryption module comprises Visual Basic script commands (Column 7 line 47 – Column 8 line 67).

Claim 32 is rejected as applied above in rejecting claim 31. Furthermore, Olkin teaches and describes, a secure messaging system for protecting the contents of an electronic message being sent to a recipient (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the confirmation message allows the sender to identify the recipient of the message (Column 13 lines 7 – 52).

Claims 35 and 40 are rejected as applied above in rejecting claims 33 and 38. Furthermore, Olkin teaches and describes, a method for sending and receiving a message to a recipient (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the encryption key is derived from the password (Column 2 lines 6 – 49 and Column 12 line 21 – Column 13 line 52).

Claims 36 and 41 are rejected as applied above in rejecting claims 33 and 38. Furthermore, Olkin teaches and describes, a method for sending and receiving a message to a recipient (Fig. 1, 7; Column 3 line 32 – Column 4 line 57 and Column 12 line 21 – Column 18 line 28), wherein the password is hashed to generate the encryption key (Column 15 lines 45 – 65 and Column 16 line 60 – Column 17 line 4).

Conclusion

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 **or faxed to:** (703) 872-9306 for all formal communications. Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy
Patent Examiner
703-305-8912
August 05, 2004

E. Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER
A/U 2136